

Secret Executive Law and UAP Programs: Force, Limits, and Access

Version 1.10 · October 2026 · nhilaw.com/issues/a2.html

Version 1.10, October 2026. Legal information, not legal advice. Published by the *Emergent Frontiers Institute* (NHI Law is not a law firm). Citations checked in October 2026; check every citation before relying on it.

Working premise. Insider accounts describe UAP retrieval and exploitation programs as resting on classified presidential directives, covert action findings, or departmental instruments that authorize conduct otherwise forbidden by statute (for example, spending appropriated funds without notice to Congress, withholding information from oversight committees, or using force against craft). This analysis assumes such instruments may exist and asks what legal force they have, what they cannot accomplish, how practitioners can obtain or test them, and how they bear on the liability of people who acted under them.

Key points

- A presidential directive has the force of an executive order whatever its form, and it lasts until revoked (24 Op. O.L.C. 29 (2000)).
 - Secrecy adds nothing to presidential power. A directive cannot authorize what a statute forbids except where the President's power is exclusive (*Youngstown*), and a covert action finding may not authorize any statutory violation (50 U.S.C. §3093(a)(5)).
 - Intelligence-funded activity must be specifically authorized by Congress (50 U.S.C. §3094(a)); for FY2024, UAP programs not reported to Congress could not be funded at all (FY2024 NDAA §1687; IAA §7343).
 - People who acted under a directive get a public-authority defense only if the authorizing official had actual authority; reliance on apparent authority survives mainly as a mens rea argument.
 - Directives can be obtained from the agencies that received them (FOIA does not reach the NSC), through MDR, and in criminal discovery (*Giffen*).
 - For a client who acted under a directive, get the text through cleared counsel before any testimony.
-

1. Summary

A presidential directive has the same legal effect as an executive order whatever its form and whether or not it is published, and it survives a change of administration until revoked. A secret

directive cannot, however, authorize what a statute forbids, except in the narrow zone where the President’s power is exclusive. For covert action, Congress has written that limit into the statute: a finding “may not authorize any action that would violate the Constitution or any statute of the United States.” 50 U.S.C. §3093(a)(5).

The consequences for UAP matters are concrete. Since the FY2024 National Defense Authorization Act, Congress has addressed UAP programs by statute: it has required reporting, required transfer of records to the National Archives, and (for FY2024) barred spending on UAP-related activities not disclosed to Congress. A classified directive purporting to authorize concealment from Congress or spending in the face of a statutory funding bar would sit in the lowest category of presidential power under *Youngstown* and would offer little protection to those who relied on it. The law instead gives individuals limited protection through the public-authority defense, which requires actual authority from an official empowered to grant it.

Access to directives is difficult but not impossible. Agencies can be compelled under FOIA to produce directives distributed to them for implementation; the presidential communications privilege does not reach such directives (*Center for Effective Government v. Department of State*, D.D.C. 2013). Agencies will argue that directives whose dissemination the White House tightly controls are not agency records. One district court accepted that argument (*EPIC v. NSA*, 988 F. Supp. 2d 1 (D.D.C. 2013)), but the D.C. Circuit vacated the holding in 2014 after the NSA released the directive (No. 13-5369, July 31, 2014), so the opinion is not precedent. The National Security Council is not an agency under FOIA (*Main Street Legal Services v. NSC*, 2d Cir. 2016). OLC opinions must be requested individually (*Campaign for Accountability v. DOJ*, D.C. Cir. 2025). Mandatory declassification review, criminal discovery in support of a public-authority defense (*United States v. Giffen*, S.D.N.Y. 2004), and congressional oversight are the other routes.

2. Instruments of secret executive law

Instrument	Source of authority	Publication	Notes
Executive orders	Art. II; statutes	Federal Register Act, 44 U.S.C. §1505(a)(1), requires publication of executive orders “except those not having general applicability and legal effect or effective only against Federal agencies or persons in their capacity as officers, agents, or employees thereof”	Classified orders and classified annexes exist
National security	Art. II	Not required to be	FAS maintains indexes

Instrument	Source of authority	Publication	Notes
directives (NSAM, NSDM, PD, NSDD, NSD, PDD, NSPD, PPD, NSPM, NSM)		published; many classified	of known directives; numbering resets with administrations (two series of NSPMs)
Covert action findings and memoranda of notification	50 U.S.C. §3093	Reported to intelligence committees (Gang of Eight in limited cases)	Statute bars findings that authorize unlawful action
OLC opinions	28 U.S.C. §§511-513; 28 C.F.R. §0.25	Discretionary	Treated as binding within the executive branch; many national security opinions classified
Classified annexes to authorization and appropriations acts	Congress	Classified schedules referenced in public law	“Secret law” made by Congress (Rudesill)
Department of Defense SAP instruments	10 U.S.C. §119; DoDD/DoDM 5205.07	Not published	Create unacknowledged and waived SAPs; govern access
Security classification guides	EO 13526 §2.2	Often classified	FY2026 NDAA required AARO to account for UAP-related guides
Historical UAP reporting rules	JANAP 146 (CIRVIS); AFR 200-2 (1953, 1954); AFR 80-17	Published, later rescinded	Documented and authentic

A current example of classified executive rules governing UAP is the set of “classified policy parameters” for engaging unidentified aerial objects announced after the February 2023 shootdowns. The President said they would be shared with Congress and “remain classified so we don’t give our roadmap to our enemies,” and that they “will guide what actions we will take while responding to unmanned and unidentified aerial objects.” Remarks on the United States Response to Unidentified Aerial Objects in North American Airspace (Feb. 16, 2023). They are the kind of directive an MDR or FOIA request ([Form A2-1](#)) should name specifically.

JANAP 146, the joint U.S.-Canadian procedure for “Communication Instructions for Reporting Vital Intelligence Sightings” (CIRVIS), is the clearest historical example of a published military directive reaching civilians. It applied to U.S. and Canadian civil and commercial aircraft and merchant and

fishing vessels (§102.b), required reports of “unidentified flying objects” among other sightings (§201), and warned in its security section that the reports “contain information affecting the National Defense” and that “[a]ny person who makes an unauthorized transmission or disclosure of such a report may be liable to prosecution under Title 18 of the US Code, Chapter 37” (§208). The warning did not itself create a crime; any prosecution would have had to satisfy 18 U.S.C. §793 or another Chapter 37 offense. The edition released by NSA refers to Department of Transportation air route traffic control centers, so it postdates 1967; the edition letter is illegible on the scan.

Documents such as the “Majestic 12” papers are of disputed authenticity (the FBI’s online Vault labels its file on them “completely bogus”). Practitioners should not rely on them as evidence of any legal instrument.

3. Legal force of a secret directive

3.1 Form and duration

The Office of Legal Counsel has concluded that a presidential directive and an executive order have the same legal effect: “It is the substance of the presidential action that is determinative, not the form of the document conveying that action.” Both “remain effective upon a change in administration, unless otherwise specified in the document, and both continue to be effective until subsequent presidential action is taken.” *Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order*, 24 Op. O.L.C. 29, 29 (2000) (headnote). The opinion (by Acting Assistant Attorney General Randolph Moss, Jan. 29, 2000) states that “there is no substantive difference in the legal effectiveness of an executive order and a presidential directive that is styled other than as an executive order,” and that a directive “would not automatically lapse upon a change of administration.” *Id.* at 29. A directive issued decades ago therefore continues in force unless revoked, which matters if UAP programs rest on old instruments.

3.2 A President may depart from his own published orders without notice

On December 7, 2007, Senator Sheldon Whitehouse read on the Senate floor three propositions he had had declassified from secret OLC opinions, “as accurately as my note-taking could reproduce them.” The first: “An Executive order cannot limit a President. There is no constitutional requirement for a President to issue a new Executive order whenever he wishes to depart from the terms of a previous Executive order. Rather than violate an Executive order, the President has instead modified or waived it.” The second: “The President, exercising his constitutional authority under article II, can determine whether an action is a lawful exercise of the President’s authority under article II.” The third: “The Department of Justice is bound by the President’s legal determinations.” 153 Cong. Rec. S15011-12 (daily ed. Dec. 7, 2007). Senators Feingold and Whitehouse proposed legislation requiring public notice when the President modifies or waives a published order, and the Senate Judiciary Committee’s Constitution Subcommittee held a hearing on “secret law” on April 30, 2008. The practical point is that published executive orders, including EO 12333 on intelligence activities and EO 13526 on classification, may not describe the rules actually in force for a given program.

3.3 Limits: statutes and *Youngstown*

Under Justice Jackson’s framework in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (concurring opinion), presidential power is at its lowest when the President acts against the express or implied will of Congress. In that category, the President may rely only on powers that Congress cannot regulate. *See also Medellín v. Texas*, 552 U.S. 491, 524-25 (2008); *Zivotofsky v. Kerry*, 576 U.S. 1, 10 (2015) (recognition power exclusive). A secret directive has no greater force than a published one; secrecy adds nothing to the President’s constitutional power.

Congress has legislated on the specific subject of UAP programs. Relevant enactments include:

- 50 U.S.C. §3373b (FY2023 NDAA §1673), authorizing disclosures to AARO notwithstanding nondisclosure agreements and other restraints, and protecting those who make them from reprisal;
- FY2024 NDAA §1687 (Pub. L. 118-31), barring the use of funds for UAP-related activities, including retrieval and reverse engineering, that were not reported to the appropriate committees and to AARO (the FY2025 NDAA did not renew it);
- FY2024 NDAA §§1841-1843 (44 U.S.C. §2107 note), requiring agencies to identify and transmit UAP records to the National Archives;
- 50 U.S.C. §3091 (duty to keep the intelligence committees “fully and currently informed”);
- 10 U.S.C. §119 (reports to Congress on special access programs, including waived programs);
- 50 U.S.C. §3094(a), under which appropriated funds available to an intelligence agency “may be obligated or expended for an intelligence or intelligence-related activity only if” they “were specifically authorized by Congress for use for such intelligence or intelligence-related activities” (or come from the CIA Reserve for Contingencies under stated conditions). An intelligence-funded UAP program that was never specifically authorized was funded unlawfully whatever a classified directive said, and no directive can cure that.

The Constitution adds its own requirement: “a regular Statement and Account of the Receipts and Expenditures of all public Money shall be published from time to time” (art. I, §9, cl. 7). The Supreme Court held that a taxpayer lacked standing to enforce the clause against the secrecy of the CIA budget, describing the matter as “committed to the surveillance of Congress.” *United States v. Richardson*, 418 U.S. 166, 179 (1974). The clause is therefore enforced by Congress, which is one more reason the funding statutes above, and not litigation, are the practical check on a secret program ([Issue D1](#)).

A directive that purported to authorize concealment of a UAP program from the committees, or spending in the face of §1687, would fall in *Youngstown*’s third category. The government’s best argument would be that the President’s control of national security information, recognized in *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988), is exclusive. No court has held that Congress lacks power to legislate on access to classified information, and the 2011 CRS analysis of the classification framework notes the same point. Congress’s power over appropriations is at its strongest when it attaches conditions to spending.

3.4 Covert action

If a UAP program were structured as covert action, 50 U.S.C. §3093 would require a written presidential finding, reporting to the intelligence committees, and compliance with subsection (a) (5): a finding “may not authorize any action that would violate the Constitution or any statute of the United States.” The statute also bars retroactive findings (§3093(a)(2)). Whether retrieval or exploitation of recovered craft, or operations against UAP, would qualify as covert action depends on whether the activity is meant “to influence political, economic, or military conditions abroad” with the U.S. role unacknowledged (§3093(e)); most of the conduct insiders describe is domestic and would fall outside the definition, which leaves it subject to ordinary statutes.

3.5 Funding restrictions and the Iran-Contra precedent

The Iran-Contra prosecutions are the closest precedent for criminal accountability where officials conceal activities that violate a funding restriction. In *United States v. North*, 708 F. Supp. 375 (D.D.C. 1988), Judge Gesell refused to dismiss a charge of conspiracy to defraud the United States (18 U.S.C. §371) premised in part on concealment of activities that circumvented the Boland Amendments, which barred funding for the Nicaraguan resistance. The court rejected the argument that the case presented a political question, reasoning that the charges turned on what officials did and what they were or were not authorized to do, and left the wisdom of the foreign policy aside. The court also declined to address North’s challenge to the Boland Amendments’ constitutionality, because the White House had functioned as if it were complying with them. *Id.* at 377-78.

The congressional phase of Iran-Contra produced the other half of the precedent: John Poindexter’s convictions for obstructing Congress and making false statements to it were reversed because trial witnesses had been exposed to his immunized testimony, not because the statements were lawful. *United States v. Poindexter*, 951 F.2d 369 (D.C. Cir. 1991) (Issues B3, D3).

The FY2024 UAP funding restriction (§1687) is structurally similar to the Boland Amendments. Officials who concealed UAP spending from Congress while that restriction was in force, and who misrepresented the activity, could face a §371 defraud-clause theory of the kind upheld in *North*. Limitations periods matter: the general five-year federal period, 18 U.S.C. §3282, runs from the last overt act. [Issue D3](#) develops criminal exposure.

4. Liability of people who acted under secret directives

4.1 The public-authority defense

A defendant who acted at the request of a government official may assert a public-authority defense, noticed under Federal Rule of Criminal Procedure 12.3. Most circuits require that the official had actual authority to sanction the conduct; reliance on an official who only appeared to have authority does not suffice, although an honest belief may bear on whether the defendant had the required mens rea. *United States v. Fulcher*, 250 F.3d 244 (4th Cir. 2001) (new trial ordered where a government agent’s post-trial testimony suggested he may have led the defendant to believe his conduct was authorized; the parties had not litigated the agent’s actual authority). The D.C. Circuit’s Watergate decision in *United States v. Barker*, 546 F.2d 940 (D.C. Cir. 1976), is the case most often cited for a mistake-of-law defense based on reasonable reliance on an official’s apparent

authority, but it has no majority rationale. The two judges who voted to reverse the Fielding break-in convictions wrote separately: Judge Wilkey relied on good-faith reliance on the apparent authority of an official by citizens recruited to assist him, and Judge Merhige relied on reliance on a government official's misstatement of the law. Judge Leventhal dissented. KeyCite shows a yellow flag, and the Third Circuit declined to follow *Barker* in *United States v. Pitt* (3d Cir. Oct. 1, 1999). Counsel should cite *Barker* with that history and pair it with the circuit's own public-authority cases.

For UAP program participants, the defense turns on whether the directive or the official who invoked it had lawful power to authorize the conduct. Under §3093(a)(5) and *Youngstown*, a directive could not lawfully authorize a statutory violation; a participant would then be left with the mens rea arguments and with *Barker*-type reliance arguments where they remain available.

4.2 Discovery of secret authorizations in criminal cases

A defendant who notices a public-authority defense can obtain discovery of government documents bearing on it, including classified documents reviewed under CIPA. In *United States v. Giffen*, 379 F. Supp. 2d 337 (S.D.N.Y. 2004), a businessman charged under the Foreign Corrupt Practices Act claimed that his conduct was undertaken with the knowledge and approval of the CIA and other agencies. The court held that documents pertaining to the possible public-authority defense were discoverable, that the obligation extended to classified documents, and that it did not extend to documents of which the prosecution was unaware. This is the most practical route by which secret directives become visible in court: a prosecution of a program participant would put the authorizing instruments in issue.

4.3 Good-faith reliance on legal advice

Congress has granted statutory reliance defenses in specific settings (for example, Detainee Treatment Act of 2005 §1004, protecting officials who relied in good faith on legal advice concerning interrogation). A UAP disclosure statute or truth commission statute could include a similar provision ([Issue B3](#)). Absent such a statute, reliance on OLC advice is relevant to intent but is not a complete defense.

4.4 Immunity of the President

Trump v. United States, 603 U.S. 593 (2024), recognized immunity from criminal prosecution for a President's official acts, absolute within the President's conclusive and preclusive authority and at least presumptive for other official acts. The decision concerns the President personally. It does not extend immunity to subordinates who carry out unlawful directives, and it does not make an unlawful directive lawful.

5. Obtaining secret directives and opinions

5.1 FOIA

- **Directives distributed to agencies.** In *Center for Effective Government v. Department of State*, 7 F. Supp. 3d 16 (D.D.C. 2013), Judge Huvelle held, as a matter of first impression, that the presidential communications privilege did not protect Presidential Policy Directive 6 on

global development, which had been distributed to agencies for implementation, and ordered it released. The government did not argue that PPD-6 was not an agency record.

- **Directives controlled by the White House.** In *Electronic Privacy Information Center v. NSA*, 988 F. Supp. 2d 1 (D.D.C. 2013), Judge Howell held that NSPD-54 (cybersecurity), which had been given only to specific senior officials with dissemination beyond those with a need to know requiring White House approval, was not an “agency record” because the White House retained control. The D.C. Circuit later vacated the judgment in part as moot. 2014 WL 12596363 (D.C. Cir. July 31, 2014).
- **The National Security Council.** The NSC is not an “agency” subject to FOIA. *Main Street Legal Services, Inc. v. National Security Council*, 811 F.3d 542 (2d Cir. 2016). Requests must go to the agencies that received and implemented a directive.
- **OLC opinions.** OLC opinions are not “final dispositions” or adopted “statements of policy and interpretations” subject to FOIA’s affirmative reading-room provision, so they must be requested individually and are subject to the deliberative process and other exemptions. *Campaign for Accountability v. DOJ*, 155 F.4th 724 (D.C. Cir. 2025). An opinion that an agency has expressly adopted as its reasoning may lose deliberative protection under the “working law” doctrine. See *Electronic Frontier Foundation v. DOJ*, 739 F.3d 1 (D.C. Cir. 2014) (OLC opinion not adopted as FBI working law).
- **Exemption 1** remains available for classified directives. The official-acknowledgment doctrine ([Issue A1](#), B1) applies.

5.2 Mandatory declassification review

Executive Order 13526 §3.5 allows any person to request declassification review of a described record, with appeal to the Interagency Security Classification Appeals Panel. MDR reaches “all information classified under this order or predecessor orders” that the requester describes with enough specificity to locate, unless it is in an exempt operational file or is the subject of pending litigation (§3.5(a)), so classified directives are covered. Two features matter for directives issued by or for a President. Information originated by the *incumbent* President, Vice President, their staffs, or EOP entities that solely advise the incumbent is exempt, but the Archivist may review and declassify papers and records of *former* Presidents and Vice Presidents held under the Presidential Records Act and related statutes, with appeal from the Archivist’s decision to the Panel (§3.5(b)). MDR is also subject to the Glomar response: an agency “may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified” (§3.6(a)), and that provision applies expressly to MDR as well as FOIA. MDR therefore offers no protection from a Glomar response; its value lies in the appeal to ISCAP. A request already reviewed within two years may be answered by reference to the prior decision (§3.5(d)).

5.3 Congressional channels

50 U.S.C. §3091 and §3093 require reporting of intelligence activities and covert action to the intelligence committees; 10 U.S.C. §119 requires reports on special access programs. Members can request directives and findings, and the committees can compel testimony. The FY2026 NDAA

required AARO to account for UAP-related security classification guides, which practitioners can use to frame requests.

5.4 Litigation discovery

Civil discovery (subject to the state secrets privilege, [Issue A1](#)) and criminal discovery under CIPA and *Brady* (as in *Giffen*) can reach directives and findings that bear on claims and defenses.

6. How disclosure would affect secret directives

1. A disclosure event would likely involve rescission or declassification of the governing directives. Under EO 13526 §3.1(d), an agency head may declassify information where the public interest in disclosure outweighs the need for protection.
 2. Once a directive is declassified, its legal effect on past conduct becomes litigable: whether it was lawful, who acted under it, and whether reliance was reasonable.
 3. A disclosure statute should require publication of all directives governing UAP programs, with a review board empowered to resolve disputes (as the 2023 UAP Disclosure Act proposed for records).
 4. Practitioners advising program participants should obtain, through counsel cleared for the purpose, the text of any directive under which the client acted, before the client gives testimony to Congress, AARO, PURSUE, or any commission.
-

7. Practice checklist

- For a program participant client: identify every instrument under which the client acted (directive, finding, SAP indoctrination, contract clause); assess whether it could lawfully authorize the conduct; preserve evidence of authorization; consider a Rule 12.3 notice if charged.
 - For a requester: send FOIA requests to each implementing agency (not to the NSC); describe the directive by number, date, subject, or series; request any OLC opinion by subject and date; file MDR requests in parallel; cite *Center for Effective Government* against presidential communications privilege claims.
 - For counsel to a committee or commission: request directives, findings, SAP reports, and classification guides under §§3091, 3093 and 10 U.S.C. §119; ask whether any directive modified or waived a published executive order.
-